ExaGrid

Retention Time-Lock for Ransomware Recovery

★★★★★

ExaGrid Tiered Backup Storage

Fastest Backups.

Fastest Recoveries.

Unparalleled, Cost-effective Scale-out.

Ransomware attacks are on the rise, becoming disruptive and potentially very costly to businesses. No matter how meticulously an organization follows best practices to protect valuable data, the attackers seem to stay one step ahead. They maliciously encrypt primary data, take control of the backup application and delete the backup data.

Protection from ransomware is a primary concern for organizations today. ExaGrid offers a unique approach to ensuring that attackers cannot compromise the backup data.

The challenge is how to protect the backup data from being deleted while at the same time allow for backup retention to be purged when retention points are hit. If you retention lock all of the data, you cannot delete the retention points and the storage costs become untenable. If you allow retention points to be deleted to save storage, you leave the system open for hackers to delete all data.

ExaGrid's unique approach is called Retention Time-Lock. It prevents the hackers from deleting the backups and allows for retention points to be purged. The result is a strong data protection and recovery solution at a very low cost of storage.

ExaGrid is Tiered Backup Storage with a front-end disk-cache Landing Zone and separate Retention Tier containing all retention data. Data is written directly to the "network facing" ExaGrid disk-cache Landing Zone. Then it is tiered into a "non-network facing" long-term retention repository where it is stored as deduplicated data objects to reduce the storage cost of long-term retention data. As data is tiered to the Retention Tier, it is deduplicated and stored in a series of objects and metadata. As with other object storage systems, the ExaGrid objects and metadata never change allowing only for the creation of new objects or deletion of old objects when retention is reached.

ExaGrid's approach to ransomware allows organizations to set up a time lock period that governs the processing of any delete requests in the Retention Tier as that tier is not network facing and not accessible to hackers. The combination of a non-network facing tier, a delayed deletion for a period of time and objects that never change are the elements of the ExaGrid Retention Time-Lock solution. For example, if the time lock period for the Retention Tier is set to 10 days, then when delete requests are sent to the ExaGrid from a backup application that has been compromised or from a hacked CIFS or other communications protocols, the data in the Retention Tier is time-locked for up to 10 days against any deletion. The data in the Landing Zone will be deleted or encrypted, however, the Retention Tier data is not deleted upon an external request for the configured period of time. When a ransomware attack is identified, simply put the ExaGrid system into a new recover mode and then restore any and all backup data to primary storage. The time lock period is separate and in addition to the days, week, months and year or retention that is set by the backup application and stored by ExaGrid in the retention repository.

The solution provides a retention lock, but only for an adjustable period of time as it delays the deletes. ExaGrid chose not to implement Retention Time-Lock forever because the cost of the storage would be unmanageable. ExaGrid already has the long term backup retention so it would be redundant to have a separate store with retention lock. The 10-day default policy for delayed deletes only takes an additional 5% to 10% of storage space. ExaGrid allows the delay of deletes from 1 day to 30 days.

Recovery Process – 5 Easy Steps

- Invoke recover mode.
  - Retention Time-Lock clock is stopped with all deletes put on hold indefinitely until data recovery operation is complete.
- Contact assigned level 2 ExaGrid customer support engineer.
  - The backup administrator can carry out the recovery using the ExaGrid GUI, but since this is not a common operation, we suggest contacting ExaGrid customer support.
- Determine the time of the event so you can plan restore.
- Determine which backup on the ExaGrid completed deduplication before the event.
- Perform restore from that backup using the backup application.

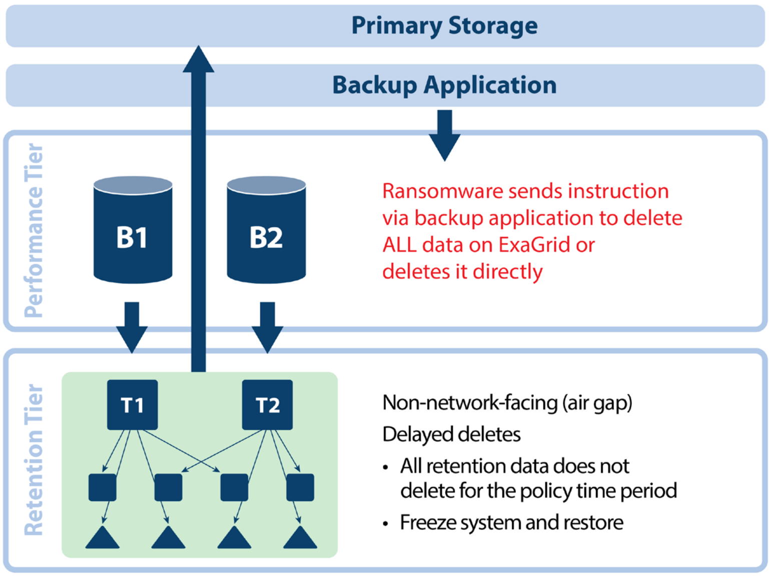
ExaGrid advantages are:

- Manage a single system instead of multiple systems for both backup storage and ransomware recovery
- Unique second Retention Tier that is only visible to ExaGrid software not to the network
- Data is not deleted as delete requests are delayed and therefore ready to recover after a ransomware attack
- Weekly, monthly, yearly and other purges still occur to keep storage costs in line with the retention periods
- The 10-day default policy for delayed deletes only takes an additional 5% to 10% of storage space
- Storage does not grow forever and stays within the backup retention period set to keep storage costs down
- All retention data is preserved and is not deleted

Example Scenarios

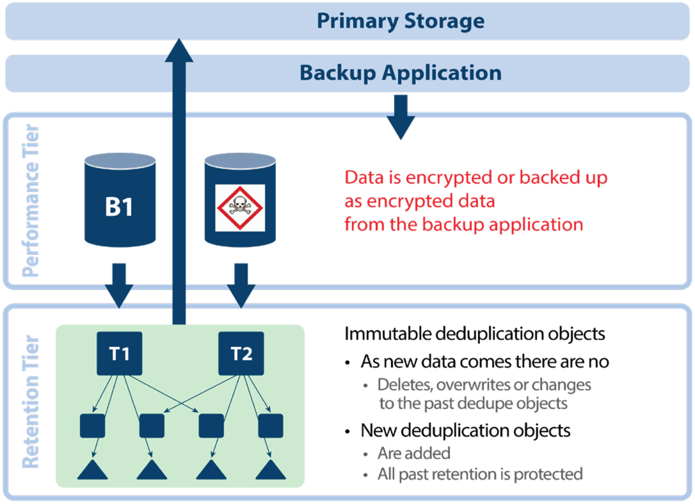
- Data is deleted in the ExaGrid disk-cache Landing Zone via the backup application or by hacking the communication protocol. Since the Retention Tier data has a delayed delete time lock, the objects are still intact and available to restore. When the ransomware event is detected, simply put the ExaGrid in a new recover mode and restore. You have as much time to detect the ransomware attack as the time lock was set for on the ExaGrid. If you had the time lock set for 10 days, then you have 10 days to detect the ransomware attack and put the ExaGrid system in the new recover mode for restoring data.

Deletion Protection of Backup Data on ExaGrid


Primary Storage
Backup Application
Performance Tier
B1
B2
Ransomware sends instruction via backup application to delete ALL data on ExaGrid or deletes it directly
Retention Tier
T1
T2
Non-network-facing (air gap)
Delayed deletes
• All retention data does not delete for the policy time period
• Freeze system and restore

- Data is encrypted in the ExaGrid disk-cache Landing Zone or is encrypted on the primary storage and backed up to ExaGrid such that ExaGrid has encrypted data in the Landing Zone and deduplicates it into the Retention Tier. The data in the Landing Zone is encrypted. However, all previously deduplicated data objects never change (immutable), so they are never impacted by the newly arrived encrypted data. ExaGrid has all previous backups before the ransomware attack that can be restored immediately. In addition to being able to recover from the most recent deduplicated backup, the system still retains all the backup data according to the retention requirements.

Encryption Protection of Backup Data on ExaGrid


Primary Storage
Backup Application
Performance Tier
B1
Data is encrypted or backed up
as encrypted data
from the backup application
Retention Tier
T1
T2
Immutable deduplication objects
• As new data comes there are no
• Deletes, overwrites or changes to the past dedupe objects
• New deduplication objects
• Are added
• All past retention is protected

Features:

- Any deletion requests are delayed by the number of days in the protection policy.
- Encrypted data written to ExaGrid does not delete or change previous backups in the repository.
- Landing Zone data that is encrypted does not delete or change previous backups in the repository.
- Set delayed deletion in 1 day increments from 0 days to 30 days.
- Protects against loss of any and all retained backups including monthlies and yearlies.
- Two-Factor Authentication (2FA) protects changes to Time-Lock setting.
  - Only Security Officer role is allowed to approve changes to Time-Lock setting.
  - 2FA with Login/Password and system generated QR code protects all accounts.
- Separate password for primary site versus second site ExaGrid.
- **Special Feature: Alarm on Delete**
  - An alarm is raised 24 hours after a large delete.
  - Alarm on large delete: A value can be set as a threshold by the backup administrator (default is 50%) and if a delete is more than the threshold, system will raise an alarm, only Admin role can clear this alarm.
  - A threshold can be configured, by individual share, based on backup pattern. (The default value is 50% for every share). When a delete request comes to the system, the ExaGrid system will honor the request and delete the data. If RTL is enabled, the data will be retained for the RTL policy (for the number of days set by an organization). When RTL is enabled, organizations will be able to recover the data using the PITR (Point-In-Time-Recovery).
  - If an organization gets false positive alarm frequently, the Admin role can adjust the threshold value from 1-99% to avoid more false alarms.